

AN - 1995-120778 [16]

AP - JP19930203747 19930727

PR - JP19930203747 19930727

TI - Coding system for facsimile - generates common key for group of subscribers and encoding and decoding is done using this key

IW - CODE SYSTEM FACSIMILE GENERATE COMMON KEY GROUP
SUBSCRIBER ENCODE

DECODE KEY

PA - (CSKC-N) CSK CORP

PN - JP7046234 A 19950214 DW199516 H04L9/06 009pp

ORD - 1995-02-14

IC - G09C1/00 ; H04L9/06 ; H04L9/14

FS - GMPI;EPI

DC - P85 W01 W02

AB - J07046234 The coding system allocates unique ID for each and every subscriber in the list. A key generation centre (1) generates a secret key for every user. The key is selected by searching a hash table, that has the index ID of the subscriber in relation to a prime number. Each and every user is provided with the complete subscriber ID list, as open information.

- Multiple users of some group, like conference members, communicate from a single user, in the same way by the system. As the system generates a common key for the group, that requires only the information of IDs of the members then the ID and secret key is transmitted. The data is encrypted by the use of the common key and transmitted. The data is decrypted at the receiver's end by the use of the common key. Thus, group of users communicate from a single user by this method.
- ADVANTAGE - Uses common key for group of members. Uses simple algorithm for encryption/decryption. Enables maintenance of security. Facilitates easy processing.
- (Dwg.1/4)

3/3 (1/1 PAJ) - (C) PAJ / JPO

PN - JP7046234 A 19950214

AP - JP19930203747 19930727

PA - CSK CORP

IN - TANAKA HATSUICHI

I - H04L9/06 ; H04L9/14 ; G09C1/00

TI - CIPHERING SYSTEM

AB - PURPOSE: To realize sophisticated security with a simple algorithm by providing a reception terminal equipment generating a secret key through specific arithmetic operation, generating a common key between a key generating center and a conference member and decoding the received ciphering text with other common key generated by the common key or the like.

- CONSTITUTION: A key generating center 1 applies unidirectional Hash

THIS PAGE BLANK (USPTO)

functions $f()$, $h()$ to each user 2 or the like based on the ID information intrinsic to user. Then a list of secret information sets P , Q , L , α , β , γ , δ , S and a public information N , subscriber ID list including a secret key G are generated by the arithmetic operation including an exponential function of a primitive element (g) of a prime. Thus, a common key is generated between the center 1 and conference membership without need of preliminary communication and the data are sent through ciphering by the common key. The receiver side generates a common key with the conference membership based on the secret key G , the ID information and the public information without need of preliminary communication and the reception terminal equipment decodes the received ciphering text.

ABV - 199505

ABD - 19950630

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-46234

(43) 公開日 平成7年(1995)2月14日

(51) Int.Cl. [*]	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/06				
9/14				
G 0 9 C 1/00		8837-5L		
			H 0 4 L 9/ 02	Z
			審査請求 未請求 請求項の数 5	F D (全 9 頁)

(21) 出願番号 特願平5-203747

(22) 出願日 平成5年(1993)7月27日

(71) 出願人 000131201

株式会社シーエスケイ

東京都新宿区西新宿2丁目6番1号

(72) 発明者 田中 初一

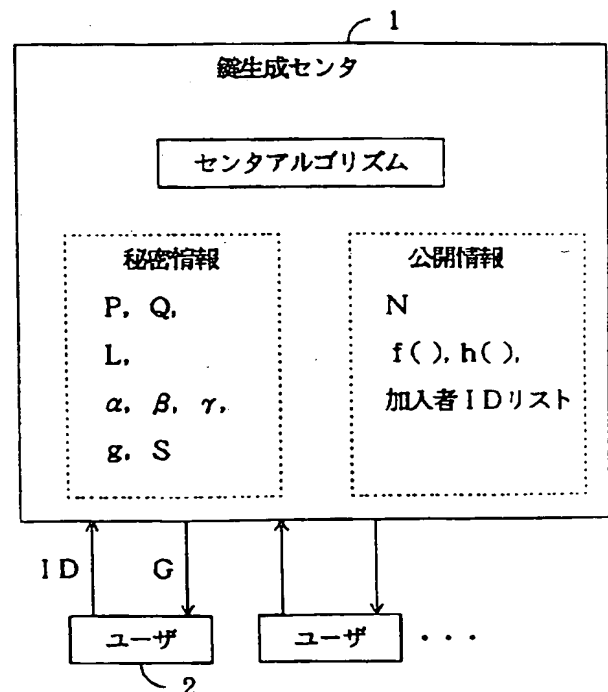
兵庫県神戸市須磨区中落合4丁目2番467
-302

(54) 【発明の名称】 暗号システム

(57) 【要約】 (修正有)

【目的】 シンプルなアルゴリズムでありながら高度のセキュリティを保ち、複数の者の間で暗号化・復号のための共通鍵を共有することができる暗号システムを提供する。

【構成】 通信に先立ち、鍵生成センタ1において、ユーザに対しその固有のID情報に基づいて一方向性ハッシュ関数の適用および素数の原始元を底とし法を用いた指数関数の適用を含む演算により秘密の鍵を生成してユーザ本人に付与する。加入者IDリストを含む所定の情報は公開情報として各ユーザに提供する。送信側端末では送信側ユーザの秘密の鍵と送信側ユーザを除く会議メンバーの公開されたID情報およびその他から予備通信を必要としないで共通鍵を生成し、この共通鍵によりメッセージを暗号化して送信する。受信側端末では受信側ユーザの秘密の鍵と受信側ユーザを除く会議メンバーの公開されたID情報およびその他から予備通信を必要としないで共通鍵を生成し、受信した暗号文を共通鍵により復号する。



【特許請求の範囲】

【請求項1】 個々のユーザに対しそのユーザ固有のID情報に基づいて一方向性ハッシュ関数の適用および素数の原始元を底とし法を用いた指数関数の適用を含む演算により秘密の鍵を生成してユーザ本人に付与すると共に、各ユーザの加入者IDリストを含む所定の情報を公開情報として提供する鍵生成センタと、

送信側ユーザの秘密の鍵と送信側ユーザを除く会議メンバーの公開されたID情報およびその他の公開情報とから送受信者間で予備通信を必要としないで会議メンバーとの間で共通鍵を生成し、この共通鍵によりメッセージを暗号化して送信する送信側端末と、

受信側ユーザの秘密の鍵と受信側ユーザを除く会議メンバーの公開されたID情報およびその他の公開情報とから送受信者間で予備通信を必要としないで共通鍵を生成し、受信した暗号文を共通鍵により復号する受信側端末とを備えたことを特徴とする暗号システム。

【請求項2】 鍵生成センタでは、

任意に選んだ2つの大きな素数P、Qに対して、 $N = PQ$

を計算してNを公開情報にし、

$L = \text{LCM}\{P-1, Q-1\} = 2\alpha\beta\gamma \quad (\text{LCM}\{\} *)$

$$K_M = (g_{Af}^{**}(\Pi_{a;M-A} I_{Af})) \cdot (g_{Ah}^{**}(\Pi_{a;M-A} I_{Ah})) \quad (\text{mod } N)$$

($\Pi_{a;M-A} I_{Af}$ は会議メンバーMから送信側ユーザAを除いた他のメンバーmの全てにつき I_{Af} を掛け合わせることを意味)により共通鍵 K_M を計算し、
受信側端末では、

$$K_M = (g_{Bf}^{**}(\Pi_{a;M-B} I_{Af})) \cdot (g_{Bh}^{**}(\Pi_{a;M-B} I_{Ah})) \quad (\text{mod } N)$$

($\Pi_{a;M-B} I_{Af}$ は会議メンバーMから受信側ユーザBを除いた他のメンバーmの全てにつき I_{Af} を掛け合わせることを意味)により共通鍵 K_M を計算することを特徴とした請求項1記載の暗号システム。

【請求項3】 α 、 β 、 γ を何らかの未知乱数でカバーして変形し、ID情報 ID_a から2つの奇数 I_{Af} 、 I_{Ah} を何らかの手法により変形して得ることを特徴とした請求項2記載の暗号システム。

【請求項4】 鍵生成センタは生成した秘密の鍵をICカードに記録して各ユーザに付与することを特徴とする請求項1、2または3記載の暗号システム。

【請求項5】 通信の開始時に作業鍵の情報を共通鍵により暗号化・復号して通信すると共に、その後は作業鍵によりメッセージを暗号化・復号して通信することを特徴とする請求項1、2、3または4記載の暗号システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明はメッセージ(電子情報)を安全に通信するための暗号システムに関するものであ

*は最小公倍数)

を満たす L 、 α および奇数 β 、 γ を求め、

P、Qの有限体 $GF(P)$ 、 $GF(Q)$ の共通の原始元 g を求め、

任意の一方向性ハッシュ関数 $f()$ 、 $h()$ を選択して公開情報にし、

ユーザmのID情報である ID_a に対し、

$$I_{Af} = 2f(ID_a) + 1$$

$$I_{Ah} = 2h(ID_a) + 1$$

10 を計算し、

$$S_a = \beta I_{Af} + \gamma I_{Ah} \quad (\text{mod } L) \quad (\text{modは法})$$

$$g_{Af} = g^{**}(\alpha S_a \beta) \quad (\text{mod } N)$$

$$g_{Ah} = g^{**}(\alpha S_a \gamma) \quad (\text{mod } N)$$

(*は左の値に対する右の値による冪乗)を計算し、
 $G_a = \{g_{Af}, g_{Ah}\}$

をユーザmに会議用鍵生成のための秘密鍵として付与し、

送信側端末では、

送信側ユーザAの秘密の鍵 g_{Af} 、 g_{Ah} と他の会議メンバーのID情報 ID_a および一方向性ハッシュ関数 $f()$ 、 $h()$ から

※受信側ユーザBの秘密の鍵 g_{Bf} 、 g_{Bh} と他の会議メンバーのID情報 ID_a および一方向性ハッシュ関数 $f()$ 、 $h()$ から

☆り、特に、ファックス等の郵便型暗号通信が可能で利用分野が広いと共に、複数の者の間で暗号化・復号のための共通鍵を共有することができる会議用鍵を用いることができるようにした暗号システムである。

【0002】

【従来の技術】「電子情報」は本質的に物質やエネルギーと異なり、

①容易にコピーが可能である。

②オリジナルとコピーの区別がない。

40 ③コピーされてもオリジナルに全くその痕跡を残さない。

という情報特有の性質があり、高度情報化社会の実現に大きく貢献すると共に、情報セキュリティの問題を発生する要因にもなるという「両刃の剣」を生み出している。

【0003】かかる情報セキュリティを実現する手法として種々のものが提案されているが、従来より実用化されている暗号システムとしては、大別して次の2つの方式が存在する。

・共通鍵暗号系

・公開鍵暗号系

【0004】共通鍵暗号系とは、暗号化する鍵（暗号化鍵）と復号する鍵（復号鍵）とが同じものをいい、予めメッセージの送信側と受信側とで安全な手段により共通の鍵を受け渡ししておき、送信側でその鍵により暗号化して送信されたものを受信側で同じ鍵で復号し、メッセージを受け取るものである。しかし、通信に先立って秘密を保った状態で鍵を引き渡す必要があるため、不便な点が多い。また、ユーザの数が多いと秘密に管理すべき鍵の数も非常に多くなり、管理が容易でないという不都合もある。

【0005】一方、公開鍵暗号系とは、ユーザ毎に暗号化鍵と復号鍵を一对ずつ作成し（任意に定めた復号鍵に対し、離散対数問題、ナップザック問題等で知られる一方向性関数により暗号化鍵を生成する。）、暗号化鍵を公開鍵リスト等で公開し、復号鍵のみを各ユーザにおいて秘密に保持しておき、送信側は受信側の公開された暗号化鍵でメッセージを暗号化して送信し、受信側では自己の復号鍵で復号を行ってメッセージを受け取るものである。なお、暗号化鍵を公開しても復号鍵が安全に保たれるのは、一方向性関数の性質に基づくものである。

【0006】この公開鍵暗号系では予め鍵を相手方と相互に持ち合う必要がないと共に、各ユーザは自己の鍵だけを持てばよいので、前述した共通鍵暗号系のような不都合はない。しかし、各ユーザの暗号化鍵を公開するための公開鍵リストを必要とすると共に、個々の公開鍵に認証機能を付与する必要がある、また、一般に公開鍵暗号系は暗号化および復号のアルゴリズムが複雑となってその演算を高速に行うのが技術的に困難であるという問題があった。

【0007】このような状況において「ID情報に基づく暗号系」が提案され、特にID情報から共通鍵を生成し、これにより暗号化・復号を行う場合には上記の公開鍵暗号系の不都合が解消されるため非常に有望である。

【0008】すなわち、ID情報に基づく暗号系では、信頼できる鍵生成センタの存在を前提とし、予め各ユーザ毎にID情報を登録すると共に、そのID情報に基づいて各ユーザに秘密の鍵を生成して付与し、各ユーザのID情報は公開する。そして、送信側のユーザは受信側のユーザの公開されたID情報およびその他の公開情報と自己の秘密の鍵とから共通鍵を生成し、これによりメッセージの暗号化を行って送信を行う。受信側のユーザは送信側のユーザの公開されたID情報およびその他の公開情報と自己の秘密の鍵とから共通鍵を生成し、これにより受信したメッセージの復号を行う。

【0009】従って、公開されるのはユーザの名前、住所、電話番号等に対応するID情報等であるため、公開鍵暗号系のように暗号化鍵を公開する方式に比べて便利かつ安全であると共に、暗号化、復号は共通鍵により行われるためアルゴリズムが簡素化できるものである。

【0010】

【発明が解決しようとする課題】このように、ID情報に基づく暗号系は非常に有効な方式であるとして種々の試みがなされているが、充分な安全性を持ったものがなく、特に複数（多数）のユーザによる結託によってセンタ秘密が解析され、任意のユーザ間の鍵が生成できてしまう等の欠点があった。

【0011】一方、本発明者は上記の欠点を解消した2者間の通信に適用できる暗号システムを既に開発し特許出願を行っているが、かかる出願においては複数の者の間で暗号化・復号のための共通鍵を共有することができる会議用鍵については考慮されていない。

【0012】本発明は上記の点に鑑み提案されたものであり、その目的とするところは、シンプルなアルゴリズムでありながら高度のセキュリティを保ち得ると共に、複数の者の間で暗号化・復号のための共通鍵を共有することができる会議用鍵を用いることができる暗号システムを提供することにある。

【0013】

【課題を解決するための手段】本発明は上記の目的を達成するため、個々のユーザに対しそのユーザ固有のID情報に基づいて一方向性ハッシュ関数の適用および素数の原始元を底とし法を用いた指数関数の適用を含む演算により秘密の鍵を生成してユーザ本人に付与すると共に、各ユーザの加入者IDリストを含む所定の情報を公開情報として提供する鍵生成センタと、送信側ユーザの秘密の鍵と送信側ユーザを除く会議メンバーの公開されたID情報およびその他の公開情報とから送受信者間で予備通信を必要としないで会議メンバーとの間で共通鍵を生成し、この共通鍵によりメッセージを暗号化して送信する送信側端末と、受信側ユーザの秘密の鍵と受信側ユーザを除く会議メンバーの公開されたID情報およびその他の公開情報とから送受信者間で予備通信を必要としないで共通鍵を生成し、受信した暗号文を共通鍵により復号する受信側端末とを備えるようにしている。

【0014】また、共通鍵の秘匿性を高めるために通信の開始時に作業鍵の情報を共通鍵により暗号化・復号して通信すると共に、その後は作業鍵によりメッセージを暗号化・復号して通信するようにすることもできる。

【0015】

【作用】本発明の暗号システムにあつては、通信に先立ち、鍵生成センタにおいて、個々のユーザに対しそのユーザ固有のID情報に基づいて一方向性ハッシュ関数の適用および素数の原始元を底とし法を用いた指数関数の適用を含む演算により秘密の鍵を生成してユーザ本人に付与する。また、各ユーザの加入者IDリストを含む所定の情報は公開情報として各ユーザに提供する。

【0016】そして、メッセージの通信に際し、送信側端末では送信側ユーザの秘密の鍵と送信側ユーザを除く会議メンバーの公開されたID情報およびその他の公開

10

20

30

40

50

情報とから予備通信を必要としないで会議メンバーとの間で共通鍵を生成し、この共通鍵によりメッセージを暗号化して送信する。また、受信側端末では受信側ユーザの秘密の鍵と受信側ユーザを除く会議メンバーの公開されたID情報およびその他の公開情報とから予備通信を必要としないで会議用共通鍵を生成し、受信した暗号文をその会議用共通鍵により復号する。

【0017】一方、通信の開始時に作業鍵の情報を共通鍵により暗号化・復号して通信すると共に、その後は作業鍵によりメッセージを暗号化・復号して通信することにより、一層、共通鍵のセキュリティを高めることができる。

【0018】

【実施例】以下、本発明の実施例につき図面を参照して*

$$N = PQ$$

を計算してNを公開情報にする。

$$L = \text{LCM}\{P-1, Q-1\} = 2\alpha\beta\gamma$$

を満たすL、 α および奇数 β 、 γ を求める。ここで、 $\text{LCM}\{P-1, Q-1\}$ は(P-1)と(Q-1)の最小公倍数を示している。

【0024】次いで、素数P、Qの有限体GF(P)、GF(Q)の共通の原始元gを求める。

【0025】次いで、任意の方向性ハッシュ関数f

$$I_{af} = 2f(ID_a) + 1 \quad (3)$$

$$I_{ah} = 2h(ID_a) + 1 \quad (4)$$

を計算する。なお、各ユーザのID情報は加入者IDリストによる公開情報とする。

$$S_a = \beta I_{af} + \gamma I_{ah} \pmod{L} \quad (5)$$

を計算する。なお、modは法(modulus)を示している。

$$g_{af} = g^{**}(\alpha S_a \beta) \pmod{N} \quad (6)$$

$$g_{ah} = g^{**}(\alpha S_a \gamma) \pmod{N} \quad (7)$$

を計算する。なお、「**」は左の値に対する右の値による冪乗を示している。すなわち、 $g^{**}(\alpha S_a \beta)$ はgの $(\alpha S_a \beta)$ 乗を意味している。

$$G_a = \{g_{af}, g_{ah}\} \quad (8)$$

をユーザmに会議用鍵生成のための秘密鍵としてICカード等に記録して付与する。

【0030】なお、 α 、 β 、 γ を何らかの未知乱数でカバーして変形し、ID情報ID_aから2つの奇数I_{af}、I_{ah}を何らかの手法により変形して得るようにすることもできる。

【0031】次に、図2は会議メンバーに属する任意のユーザ間でメッセージの通信を行う際のシステム構成の例を示したものである。

【0032】図2において、本システムは、ユーザAが他の会議メンバーであるユーザB、C、…と暗号通信を行うための送信側端末3と、有線あるいは無線による通信路4と、ユーザB、C、…がメッセージの受信を行うための受信側端末5、6、…とから構成されている。

*説明する。

【0019】図1は本発明の暗号システムにおける鍵生成センタの一実施例を示す構成図である。

【0020】図1において、鍵生成センタ1は秘密情報と公開情報とを有し、新規に加入するユーザ2に対してそのユーザの名前、住所、電話番号等に応じたID情報IDの登録を行うと共に、各情報に基づきセンタアルゴリズムにより秘密の鍵Gを付与する。なお、鍵Gは実際にはビットデータ列である。そのため、ICカード等に記録して密かに付与するのが好ましい。

【0021】以下、鍵生成センタ1における秘密情報、公開情報、センタアルゴリズムについて説明する。

【0022】まず、鍵生成センタ1では、任意に選んだ2つの大きな素数P、Qに対し、

(1)

※ 【0023】次いで、上記の素数P、Qに対し、

(2)

★()、h()を選択し、これを公開情報にする。なお、方向性ハッシュ関数としては、離散対数問題、ナップザック問題等で知られる関数が使用できる。

【0026】次いで、ユーザmのID情報であるID_aに対し、

☆ 【0027】次いで、

☆

◆ 【0028】次いで、

◆30

* 【0029】そして、上式で得られた g_{af} 、 g_{ah} を組にした、

(8)

※ 【0033】また、送信側端末3には暗号化手段31と共通鍵生成手段32とが設けられ、受信側端末5、6、…には復号手段51、61、…と共通鍵生成手段52、62、…とが設けられている。

【0034】以下、メッセージの送信および受信につき、各部の機能とともに、動作を説明する。なお、送信側端末3においてユーザAが平文(暗号化されていない状態)のメッセージを受信側端末5のユーザBに送信する場合を考える。

【0035】まず、送信側端末3の共通鍵生成手段32においては、送信側ユーザAの秘密の鍵 g_{af} 、 g_{ah} と鍵生成センタ1の公開情報から得た他の会議メンバーのID情報ID_aおよび方向性ハッシュ関数f()、h()から

※50

7

$$K_M = (g_{Af}^{**} (\Pi_{A;M-A} I_{Af})) \cdot (g_{Ah}^{**} (\Pi_{A;M-A} I_{Ah})) \pmod{N} \quad (9)$$

により共通鍵 K_M を計算する。なお、 $(\Pi_{A;M-A} I_{Af})$ は会議メンバーMから送信側ユーザAを除いた他のメンバーmの全てにつき I_{Af} をかけ合わせることを意味している。

【0036】そして、暗号化手段31は算出された共通鍵 K_M によりメッセージを暗号化し、通信路4を介して*

$$K_M = (g_{Bf}^{**} (\Pi_{A;M-B} I_{Af})) \cdot (g_{Bh}^{**} (\Pi_{A;M-B} I_{Ah})) \pmod{N} \quad (10)$$

により共通鍵 K_M を計算する。なお、 $(\Pi_{A;M-B} I_{Af})$ は会議メンバーMから受信側ユーザBを除いた他のメンバーmの全てにつき I_{Af} をかけ合わせることを意味している。

【0038】そして、復号手段51は算出された共通鍵 K_M により通信路4を介して受信した暗号文を復号し、※

$$\begin{aligned} K_M &= (g^{**} (\alpha S_A \beta \Pi_{A;M-A} I_{Af})) \\ &\quad \cdot (g^{**} (\alpha S_A \gamma \Pi_{A;M-A} I_{Ah})) \pmod{N} \\ &= g^{**} (\alpha S_A (\beta \Pi_{A;M-A} I_{Af} + \gamma \Pi_{A;M-A} I_{Ah})) \pmod{N} \\ &= g^{**} (\alpha (\beta I_{Af} + \gamma I_{Ah}) (\beta \Pi_{A;M-A} I_{Af} + \gamma \Pi_{A;M-A} I_{Ah})) \pmod{N} \\ &= g^{**} (\alpha \beta^2 I_{Af} \Pi_{A;M-A} I_{Af} \\ &\quad + \alpha \beta \gamma (I_{Af} \Pi_{A;M-A} I_{Ah} + I_{Ah} \Pi_{A;M-A} I_{Af}) \\ &\quad + \alpha \gamma^2 I_{Ah} \Pi_{A;M-A} I_{Ah}) \pmod{N} \end{aligned}$$

となる。ここで、

$$2\alpha\beta\gamma = L = 0 \pmod{L}$$

であり、 $(I_{Af} \Pi_{A;M-A} I_{Ah})$ 、 $(I_{Ah} \Pi_{A;M-A} I_{Af})$ はそれぞれ奇数となり、両者を加えたものは偶数となるため、 K_M を変形してきた最後の式の中間項は0となる。また、

$$K_M = g^{**} (\alpha (\beta^2 \Pi_{A;M} I_{Af} + \gamma^2 \Pi_{A;M} I_{Ah})) \pmod{N}$$

となる。

【0041】一方、式(10)は式(6)、(7)を g_{Bf} 、 g_{Bh} に適用し、これに式(5)を適用し、更に

$$\begin{aligned} K_M &= (g^{**} (\alpha S_B \beta \Pi_{A;M-B} I_{Af})) \\ &\quad \cdot (g^{**} (\alpha S_B \gamma \Pi_{A;M-B} I_{Ah})) \pmod{N} \\ &= g^{**} (\alpha S_B (\beta \Pi_{A;M-B} I_{Af} + \gamma \Pi_{A;M-B} I_{Ah})) \pmod{N} \\ &= g^{**} (\alpha (\beta I_{Bf} + \gamma I_{Bh}) (\beta \Pi_{A;M-B} I_{Af} + \gamma \Pi_{A;M-B} I_{Ah})) \pmod{N} \\ &= g^{**} (\alpha \beta^2 I_{Bf} \Pi_{A;M-B} I_{Af} \\ &\quad + \alpha \beta \gamma (I_{Bf} \Pi_{A;M-B} I_{Ah} + I_{Bh} \Pi_{A;M-B} I_{Af}) \\ &\quad + \alpha \gamma^2 I_{Bh} \Pi_{A;M-B} I_{Ah}) \pmod{N} \\ &= g^{**} (\alpha (\beta^2 \Pi_{A;M} I_{Af} + \gamma^2 \Pi_{A;M} I_{Ah})) \pmod{N} \end{aligned}$$

となり、両式は一致する。従って、 K_M を共通鍵暗号系の鍵として暗号化・復号することによりメッセージの暗号通信を行うことができる。

【0042】一方、本システムのセキュリティがどうして高いかを示す必要があるが、暗号システムが絶対に安全であるということは理論的には証明できない。すなわち、アタック(暗号解析)が可能であることが証明され

8

*受信側端末5に送信する。

【0037】一方、受信側端末5の共通鍵生成手段52においては、受信側ユーザBの秘密の鍵 g_{Bf} 、 g_{Bh} と鍵生成センタ1の公開情報から得た他の会議メンバーのID情報ID。および一方向性ハッシュ関数 $f()$ 、 $h()$ から

※平文のメッセージを得る。

【0039】なお、式(9)、(10)により求めた共通鍵 K_M が互いに等しいことは次のようにして証明できる。

【0040】式(9)は式(6)、(7)を g_{Af} 、 g_{Ah} に適用し、更に式(5)を適用すると、

$$\star I_{Af} \Pi_{A;M-A} I_{Af} = \Pi_{A;M} I_{Af}$$

$$I_{Ah} \Pi_{A;M-A} I_{Ah} = \Pi_{A;M} I_{Ah}$$

となる。なお、 $(\Pi_{A;M} I_{Af})$ は会議メンバーMのメンバーmの全てにつき I_{Af} をかけ合わせることを意味している。 $(\Pi_{A;M} I_{Ah})$ についても同様である。よって、

★30

$$\star 2\alpha\beta\gamma = L = 0 \pmod{L}$$

を適用すると、

☆

◆ないことが、安全性の証明になる。ただし、定性的にセキュリティの高さの根拠を示せば次のようになる。

【0043】①式(1)においてNは公開情報であるが、このNから素数P、Qを算出することは計算量的に不可能である。

【0044】②式(2)により生成される秘密情報 α 、 β 、 γ は素数P、Qからそれぞれ1を引いたものの

最小公倍数およびその素因数であるため、 N の素因数分解が分からない限り公開情報から割り出すことは殆ど不可能であり、これらを各所の式に用いているため、値の不規則性が高く、種々の数学的手法による解析が適用しにくい。

【0045】③素数 P 、 Q の有限体 $GF(P)$ 、 $GF(Q)$ の共通の原始元 g はそれ自体が公開情報から割り出されることは殆ど不可能であり、これを式の途中に用いているため、値の不規則性が高く、種々の数学的手法による解析が適用しにくい。

【0046】④式(3)、(4)において一方向性ハッシュ関数 $f()$ 、 $h()$ を用いているため、逆方向の数学的解析は殆ど不可能である。

【0047】⑤式(6)、(7)において原始元 g の冪乗(指数)および N の法を用いているため、逆方向の数学的解析はほとんど不可能である。従って、ユーザが自己の秘密の情報を用い、あるいは複数のユーザが結託してそれぞれの秘密の情報を提供し合っても、センタ秘密を解析することは殆ど不可能である。

【0048】次に、図3は本発明の他の実施例を示したものであり、より共通鍵ならびにメッセージのセキュリティを高めたものである。なお、鍵生成センタ1の構成および動作は前述したものと同様である。

【0049】図3においては、図2の構成に比して、送信側端末3に作業鍵保持手段33と鍵切換手段34が付加され、受信側端末5、6、…にも作業鍵保持手段53、…と鍵切換手段54、…が付加されている。

【0050】動作にあたり、送信側端末3においてユーザAが平文(暗号化されていない状態)のメッセージを受信側端末5のユーザBに送信する場合は次のようになる。

【0051】まず、送信側端末3の共通鍵生成手段32においては、送信側ユーザAの秘密の鍵 g_{Af} 、 g_{Ah} と鍵生成センタ1の公開情報から得た他の会議メンバーのID情報ID_mおよび一方向性ハッシュ関数 $f()$ 、 $h()$ から共通鍵 K_m を計算する。

【0052】これとはほぼ同時に、作業鍵保持手段33はユーザAから与えられた任意の作業鍵 K_w を保持し、通信開始時のメッセージとして暗号化手段31に与えると共に、鍵切換手段34にも与える。

【0053】鍵切換手段34は通信の開始時の一定期間は共通鍵生成手段32からの共通鍵 K_m を通過させて暗号化手段31に与え、一定期間の経過後は作業鍵保持手段33からの作業鍵 K_w を暗号化手段31に与える。

【0054】従って、暗号化手段31は通信の開始時の一定期間は共通鍵 K_m を暗号化鍵として用い、作業鍵 K_w の情報をメッセージとして送信する。

【0055】受信側端末5でも同様に共通鍵生成手段52が共通鍵 K_m を生成し、鍵切換手段54は通信の開始時においてはこの共通鍵 K_m を復号手段51に与えてい

る。

【0056】従って、通信路4を介して送信側端末3から送られてきた作業鍵 K_w の暗号化されたメッセージは共通鍵 K_m により復号手段51が復号し、これを作業鍵保持手段53が保持する。

【0057】そして、作業鍵 K_w の情報が受信側端末5に完全に伝わった後、両端末3、5の鍵切換手段34、54は暗号化手段31に与える暗号化鍵を作業鍵 K_w に切り換え、その後は本来送信したいメッセージを作業鍵 K_w を用いて暗号化、復号して通信する。従って、暗号文は図4に示すような状態となる。なお、作業鍵 K_w は任意に設定できると共に、通信の途中で自由に変更することもできる。

【0058】この実施例の場合、ユーザA、B、C、…を含む会議メンバーMの間では一つしかない共通鍵 K_m を通信開始時の短時間しか使用せず、その後は任意の作業鍵 K_w を使って通信が行えるため、共通鍵ならびにメッセージのセキュリティをより一層向上させることができる。

【0059】

【発明の効果】以上説明したように、本発明の暗号システムにあつては、ID情報に基づく暗号系を基本として、ファックスのような郵便型の暗号通信を可能にし、また、アタック(暗号破り)を防止するための種々の工夫を加えているため、シンプルで高度のセキュリティを保ち得るという効果がある。更に、複数の者の間で共有できる会議用鍵を用いることができるため、同じ内容のメッセージを複数の者に送信する場合に送信が1回で済み、処理が容易になるという効果がある。

【図面の簡単な説明】

【図1】本発明の暗号システムにおける鍵生成センタの一実施例を示す構成図である。

【図2】本発明の暗号システムにおける送信側および受信側の端末の一実施例を示す構成図である。

【図3】本発明の暗号システムにおける送信側および受信側の端末の他の実施例を示す構成図である。

【図4】図3の実施例における暗号文の論理的構成を示す図である。

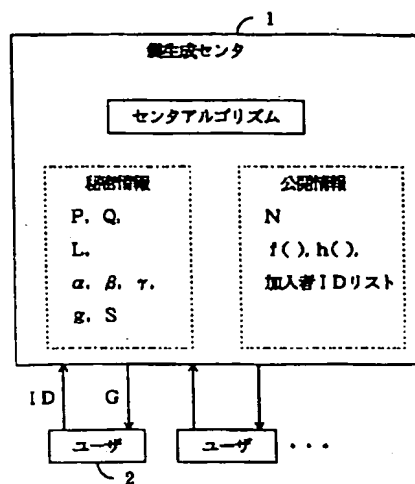
【符号の説明】

- 1……鍵生成センタ
- 2……ユーザ
- 3……送信側端末
- 31…暗号化手段
- 32…共通鍵生成手段
- 33…作業鍵保持手段
- 34…鍵切換手段
- 4……通信路
- 5……受信側端末
- 51…復号手段

52...共通鍵生成手段
 53...作業鍵保持手段
 54...鍵切換手段

11

【図1】



6...受信側端末
 61...復号手段
 62...共通鍵生成手段

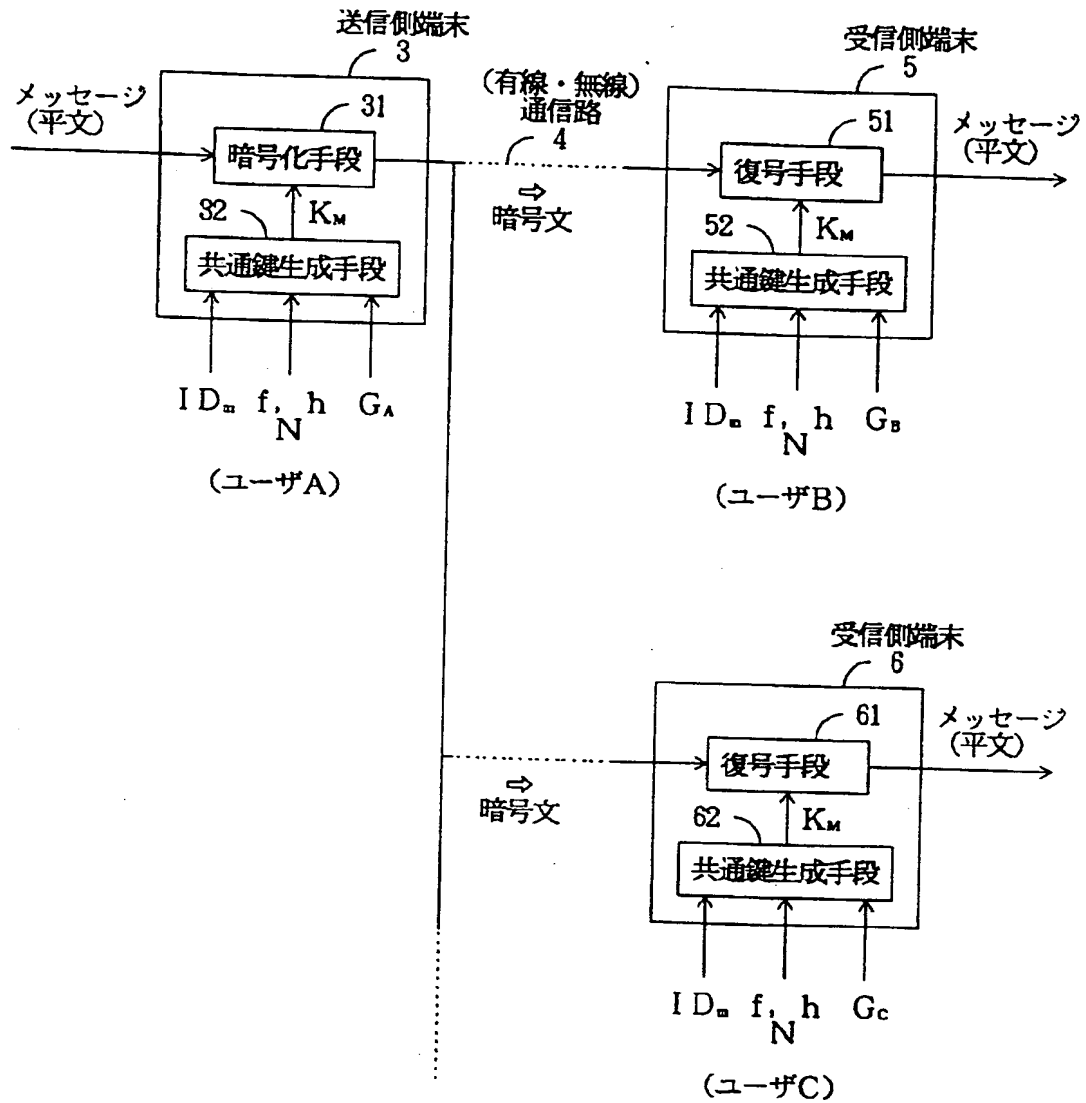
12

【図4】

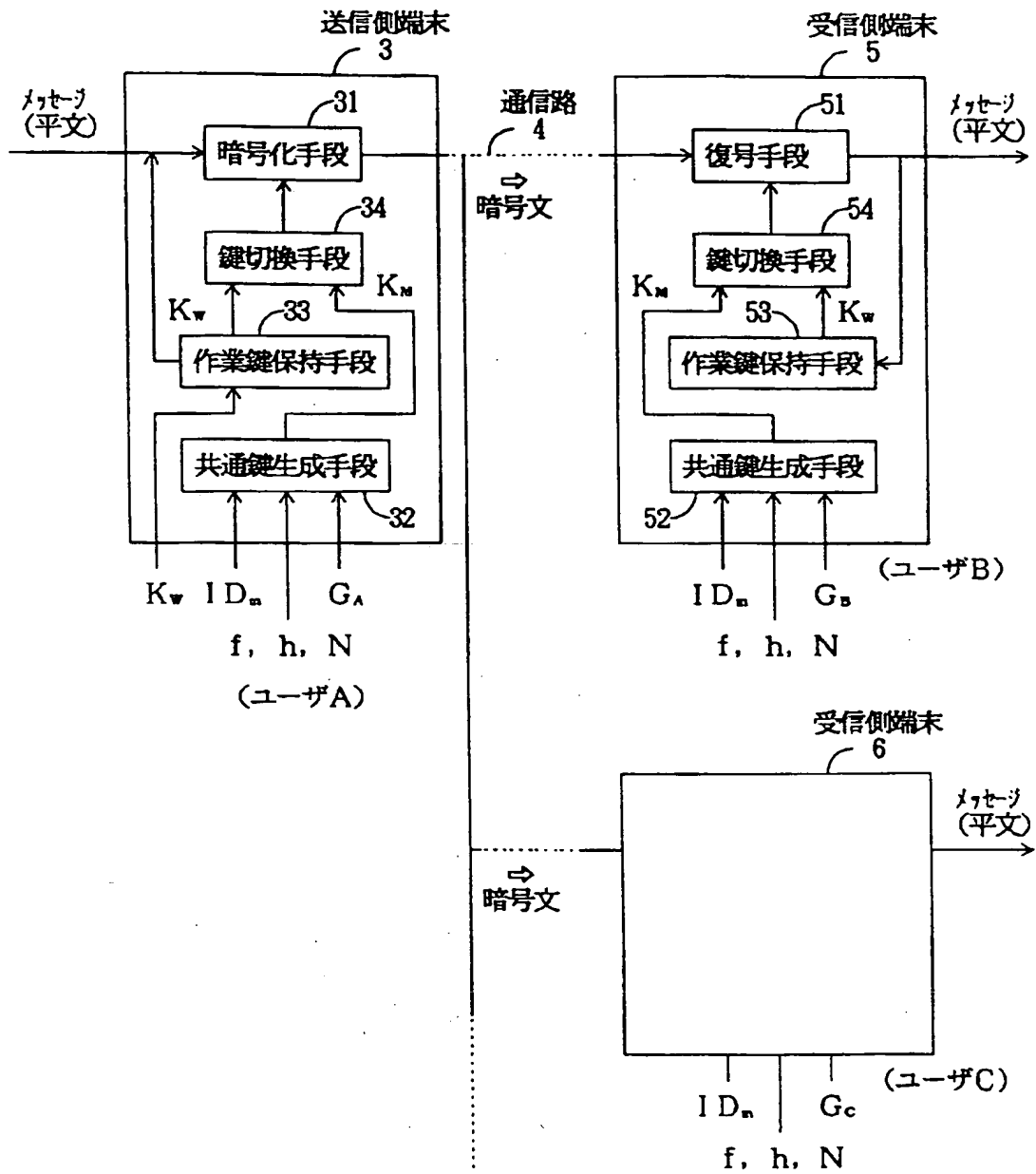
暗号文

K_w についての情報 (K_w で暗号化)	メッセージ (K_w で暗号化)
--------------------------------	------------------------

【図2】



【図3】



THIS PAGE BLANK (USPTO)